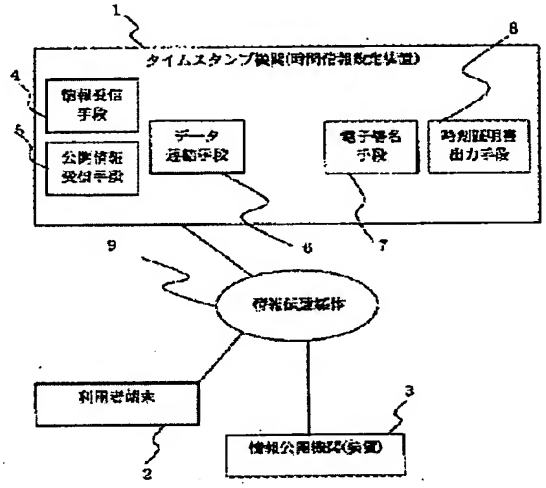
TIME INFORMATION SETTING DEVICE AND TIME CERTIFICATION VERIFICATION DEVICE

Patent number: JP2002215825
Publication date: 2002-08-02
Inventor: MIYAZAKI KAZUYA; KAMOSHITA AKITERU; TOGASHI MASATAKA
Applicant: MITSUBISHI ELECTRIC CORP
Classification:
- international: *G09C1/00;* **G09C1/00**; (IPC1-7): G06F17/60; G09C1/00
- european:
Application number: JP20010007507 20010116
Priority number(s): JP20010007507 20010116

Report a data error here

Abstract of **JP2002215825**

PROBLEM TO BE SOLVED: To provide a technology to make impossible to set up the certification time before the time to be certified in connection with a time information setting device setting up certification time to material objects and information and the time certification verification device verifying the certification time. SOLUTION: A data connecting means 6 connects information received by an information receiving means 1 and open information (information not predictable beforehand; e.g. news, stock price or the like) received by an open information receiving means 5, creates a time certificate by adding an electronic signature by an electronic signature means 7 and outputs the created time certificate by a time certificate output means 8.



Data supplied from the ***esp@cenet*** database - Worldwide

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－215825
（P2002－215825A）
(43)公開日　平成14年８月２日(2002.8.2)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　17/60	１４０	Ｇ０６Ｆ　17/60	１４０	５Ｊ１０４
	ＺＥＣ		ＺＥＣ	
	３０２		３０２Ｅ	
	５１２		５１２	
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｚ	

審査請求　未請求　請求項の数９　ＯＬ　（全９頁）

(21)出願番号　特願2001－7507(P2001－7507)

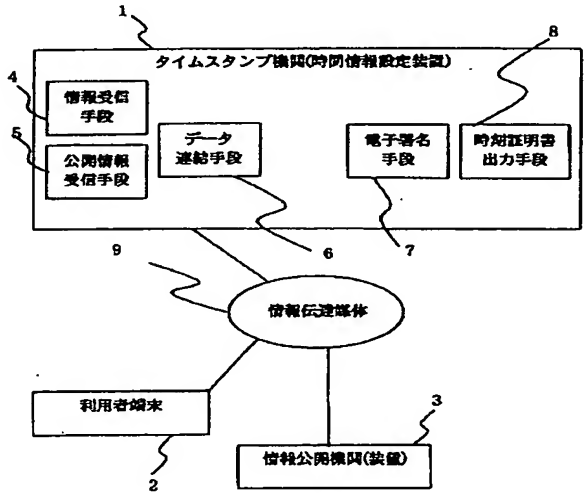
(22)出願日　平成13年１月16日(2001.1.16)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　宮崎　一哉
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(72)発明者　鴨志田　昭輝
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100099461
弁理士　溝井　章司　（外２名）

最終頁に続く

(54)【発明の名称】　時間情報設定装置及び時刻証明検証装置

(57)【要約】
【課題】　有体物や情報に対して証明時刻を設定する時間情報設定装置および、その証明時刻を検証する時刻証明検証装置に係り、証明時刻以前にその証明時刻を設定できないようにする技術を提供することを課題とする。
【解決手段】　データ連結手段６は、情報受信手段１で受信した情報と、公開情報情報受信手段５で受信した公開情報（例えば、ニュースや株価情報などの事前に予測できない情報）とを連結し、更に、電子署名手段７により、電子署名を付加することにより時刻証明書を生成し、生成した時刻証明書を時刻証明書出力手段８より出力する。



【特許請求の範囲】

【請求項１】　事前に予期できない事象についての公開情報を送信する情報公開機関装置に接続する時間情報設定装置であって、以下の要素を有することを特徴とする時間情報設定装置（１）時刻証明の対象となる対象情報を受信する情報受信手段、（２）情報公開機関装置から、上記公開情報を受信する公開情報受信手段、（３）受信した上記対象情報と、受信した上記公開情報とを連結し、連結したデータを生成するデータ連結手段、（４）上記連結したデータに電子署名を付加する電子署名手段、（５）上記連結したデータと、付加された上記電子署名とを含む時刻証明情報を出力する時刻証明書出力手段。

【請求項２】　上記データ連結手段は、上記対象情報と、上記公開情報とに加えて、更に、証明する日時を示す日時情報を連結することを特徴とする請求項１記載の時間情報設定装置。

【請求項３】　事前に予期できない事象についての公開情報を送信する情報公開機関装置に接続する時間情報設定装置であって、以下の要素を有することを特徴とする時間情報設定装置（１）時刻証明の対象となる対象情報を受信する情報受信手段、（２）情報公開機関装置から、上記公開情報を受信する公開情報受信手段、（３）受信した上記対象情報を縮約し、縮約した上記対象情報と、受信した上記公開情報と、証明する日時を示す日時情報とを連結し、連結したデータを生成するデータ連結手段、（４）上記連結したデータに電子署名を付加する電子署名手段、（５）上記連結したデータと、付加された上記電子署名とを含む時刻証明情報を出力する時刻証明書出力手段、（６）上記連結したデータを公開する情報公開手段。

【請求項４】　上記情報公開手段は、上記連結したデータを縮約し、縮約したデータを公開することを特徴とする請求項３記載の時間情報設定装置。

【請求項５】　事前に予期できない事象についての公開情報を送信する情報公開機関装置に接続する時間情報設定装置であって、以下の要素を有することを特徴とする時間情報設定装置（１）情報公開機関装置から、上記公開情報を受信する公開情報受信手段、（２）受信した上記公開情報と、証明する日時を示す日時情報とを連結し、連結したデータを生成するデータ連結手段、（３）上記連結したデータに電子署名を付加する電子署名手段、（４）上記連結したデータと、付加された上記電子署名とを表わす印刷形態を生成する時刻証明フォーマット生成手段、（５）生成した印刷形態を印刷する印刷手段。

【請求項６】　上記印刷手段は、貼り換えできないシールに印刷することを特徴とする請求項５記載の時間情報設定装置。

【請求項７】　上記印刷手段は、時刻証明の対象となる物品に直接印刷することを特徴とする請求項５記載の時間情報設定装置。

【請求項８】　以下の要素を有することを特徴とする時刻証明検証装置（１）事前に予期できない事象についての公開情報と、証明する日時を示す日時情報と連結した連結データと、上記連結データに付加された電子署名とを表わす印刷形態を読み取る読み取り手段、（２）読み取った印刷形態に表わされている上記連結データと上記電子署名の検証を行う検証手段、（３）検証結果を出力する出力手段。

【請求項９】　上記出力手段は、上記検証結果と併せて、検証の対象となる商品の価格情報と、商品の名称とを印刷することを特徴とする請求項８記載の時刻証明検証装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】この発明は、有体物や情報に対する時刻の設定および検証方法に関するものである。より詳しくは、ソフトウェア、データ、情報、あるいは製品に対して、生成、保存等の事象が発生した時刻あるいは存在している時刻を保証するための時刻の設定および検証方法に関するものである。

【０００２】

【従来の技術】図１２は、例えば、特表平６－５０１５７１に示された従来のタイムスタンプ方式のフローチャートを示している。図１２に基づいて従来の時間情報設定及び検証方式の動作を説明する。まず、著者が時刻情報の設定対象である数値文書（デジタルデータのこと）を用意する（ステップＳ１００１）。次にその文書のハッシュを生成し（ステップＳ１００２）、そのハッシュを時刻情報を設定するタイムスタンプ機関に送信する（ステップＳ１００３）。すると、タイムスタンプ機関はそのハッシュと時刻データを連結した受理書を作成し（ステップＳ１００４）、その受理書と現在の連鎖値を連結する（ステップＳ１００５）。次に、タイムスタンプ機関は受理書と現在の連鎖値を連結したデータのハッシュを生成して新しい連鎖値とし（ステップＳ１００６）、その新しい連鎖値を記した証明書を著者に送る（ステップＳ１００７）。

【０００３】従来の時間情報設定および検証法式は、上記のように連鎖値を利用して時刻情報を設定するものであったため、文書を登録した順序の改ざんが困難となり、文書登録順序は保証されることになる。しかし、証明書に表される時刻そのものの正当性を保証するものではない。つまり、時系列順にならべられた文書に対する時刻が揃って大きく前後にずれている可能性を否めないという問題点があった。

【０００４】また、時刻を表すデータは一般に時刻を示す数値あるいは文字列で与えられるため、利用者に対して直感的にそれが正確な時刻であることを認識させられ

るものではない。つまり、基となる時計が狂っているかもしれない、あるいは時刻を示す数値や文字列に誤植があるかもしれないと思わせる可能性があるという問題点があった。

【０００５】

【発明が解決しようとする課題】この発明は上記のような問題点を解決するためになされたもので、時刻の保証、特に時刻情報を生成する際に、時刻情報を生成する正にその時刻において、その時刻以降の時刻を表す時刻情報を生成できないことを保証することを目的とする。また、時刻情報が表している時刻が、利用者に対して直感的にその当時の正しい時刻であることを認識させ易いものとすることを目的とする。これにより、時刻の不正刻印表示を防止し、時刻データとしての正確性の確保が可能となり、例えば、生鮮食料品の製造、発送、鶏卵の産出時刻、発送、調理品の製造、あるいは情報の生成あるいは登録等に対し時刻を偽ることを防止する。

【０００６】

【課題を解決するための手段】この発明に係る時間情報設定装置は、事前に予期できない事象についての公開情報を送信する情報公開機関装置に接続する時間情報設定装置であって、以下の要素を有することを特徴とする。（１）時刻証明の対象となる対象情報を受信する情報受信手段、（２）情報公開機関装置から、上記公開情報を受信する公開情報受信手段、（３）受信した上記対象情報と、受信した上記公開情報とを連結し、連結したデータを生成するデータ連結手段、（４）上記連結したデータに電子署名を付加する電子署名手段、（５）上記連結したデータと、付加された上記電子署名とを含む時刻証明情報を出力する時刻証明書出力手段。

【０００７】上記データ連結手段は、上記対象情報と、上記公開情報とに加えて、更に、証明する日時を示す日時情報を連結することを特徴とする。

【０００８】この発明に係る時間情報設定装置は、事前に予期できない事象についての公開情報を送信する情報公開機関装置に接続する時間情報設定装置であって、以下の要素を有することを特徴とする。（１）時刻証明の対象となる対象情報を受信する情報受信手段、（２）情報公開機関装置から、上記公開情報を受信する公開情報受信手段、（３）受信した上記対象情報を縮約し、縮約した上記対象情報と、受信した上記公開情報と、証明する日時を示す日時情報とを連結し、連結したデータを生成するデータ連結手段、（４）上記連結したデータに電子署名を付加する電子署名手段、（５）上記連結したデータと、付加された上記電子署名とを含む時刻証明情報を出力する時刻証明書出力手段、（６）上記連結したデータを公開する情報公開手段。

【０００９】上記情報公開手段は、上記連結したデータを縮約し、縮約したデータを公開することを特徴とする。

【００１０】この発明に係る時間情報設定装置は、事前に予期できない事象についての公開情報を送信する情報公開機関装置に接続する時間情報設定装置であって、以下の要素を有することを特徴とする。（１）情報公開機関装置から、上記公開情報を受信する公開情報受信手段、（２）受信した上記公開情報と、証明する日時を示す日時情報とを連結し、連結したデータを生成するデータ連結手段、（３）上記連結したデータに電子署名を付加する電子署名手段、（４）上記連結したデータと、付加された上記電子署名とを表わす印刷形態を生成する時刻証明フォーマット生成手段、（５）生成した印刷形態を印刷する印刷手段。

【００１１】上記印刷手段は、貼り換えできないシールに印刷することを特徴とする。

【００１２】上記印刷手段は、時刻証明の対象となる物品に直接印刷することを特徴とする。

【００１３】この発明に係る時刻証明検証装置は、以下の要素を有することを特徴とする。（１）事前に予期できない事象についての公開情報と、証明する日時を示す日時情報と連結した連結データと、上記連結データに付加された電子署名とを表わす印刷形態を読み取る読み取り手段、（２）読み取った印刷形態に表わされている上記連結データと上記電子署名の検証を行う検証手段、（３）検証結果を出力する出力手段。

【００１４】上記出力手段は、上記検証結果と併せて、検証の対象となる商品の価格情報と、商品の名称とを印刷することを特徴とする。

【００１５】

【発明の実施の形態】実施の形態１．図１は、実施の形態１におけるブロック図である。図１において、１は、利用者からの時刻証明情報の設定要求に応えて要求された情報に対して時刻証明情報を生成し、発行するタイムスタンプ機関（時間情報設定装置）、２は、タイムスタンプ機関１に対してある情報に対する時刻証明情報を要求する利用者端末、３は、タイムスタンプ機関１が時刻証明情報を作成するときに利用する公開情報を発行する情報公開機関（装置）、４は、利用者端末２から送られてくる情報であって、時刻保証情報を発行する対象となる情報（対象情報）を受信する情報受信手段、５は、情報公開機関３が発行した公開情報を受信する公開情報受信手段、６は、情報受信手段４が受信した情報と公開情報受信手段５が受信した公開情報を連結するデータ連結手段、７は、データ連結手段６が連結したデータに電子署名を付加する電子署名手段、８は、電子署名手段７により得られた電子署名と縮約されたデータを含む時刻証明書を利用者端末２に向けて出力する時刻証明出力手段、９は、タイムスタンプ機関１と利用者端末２と情報公開機関（装置）３の間で情報を交換するための情報伝達媒体（例えば、インターネットのようなネットワークを含む）である。

【００１６】次に動作について説明する。まず、ある情報に対する時刻証明を得たい利用者が、利用者端末２から情報伝達媒体１０を通して、タイムスタンプ機関１に対して情報あるいはそのメッセージ縮約を伴ったタイムスタンプ要求を送付する。

【００１７】タイムスタンプ要求を受け取ったタイムスタンプ機関１は、情報公開機関３より受け取った公開情報を利用して時刻証明書を作成し、それを利用者端末２に送信する。

【００１８】上記動作のうち、特に、タイムスタンプ機関１における動作の詳細をフローチャートに基づいて説明する。図２は、実施の形態１におけるタイムスタンプ機関の動作を示すフローチャートである。まず、情報受信手段４により、利用者から時刻証明の対象となる情報ｄを取得する（ステップ１０１）。時刻証明の対象となる情報は、文書、動画、静止画、音声などを表すバイナリデータである。

【００１９】その直後あるいは同時に公開情報受信手段５により情報公開機関３が発行した公開情報ｐを取得する（ステップ１０２）。公開情報は、文書、動画、静止画、音声などを表すバイナリデータであり、時々刻々と変化する自然現象や社会現象に伴うものであり、事前に予期できない情報である。例えば、通信社によるニュース速報、株価情報、為替レート、ＴＶ放送、ラジオ放送、気象情報、気象衛星による雲の画像などを表すデータであり、そのデータを示すと日時が特定できることが条件となる。即ち、公開情報ｐの表す事象の日時ｔが周知であったり、情報公開機関３に日時ｔを照会できるなど、公開情報ｐから日時ｔが直ちに得られるものとする。このような公開情報のうち、最新のものを受信し、使用する。

【００２０】次にステップ１とステップ２で得たデータをデータ連結手段６により連結し（ステップ１０３）、電子署名手段７によりそのデータ（ｄ＋ｐ）に対するタイムスタンプ機関１の電子署名Ｓｔ（ｄ＋ｐ）を生成する（ステップ１０４）。電子署名の方法は、ＭＤ２やＭＤ５等のアルゴリズムによりデータのハッシュ値をとり、その値をＲＳＡ公開鍵暗号系の秘密鍵で暗号化するなどによる。

【００２１】そして、連結したデータ（ｄ＋ｐ）と電子署名Ｓｔ（ｄ＋ｐ）を含む、情報ｄに対する時刻ｔの時刻証明書Ｃｔ（ｄ）を生成／出力する（ステップ１０５）。図３は、実施の形態３における時刻証明書Ｃｔ（ｄ）の構成を示す図である。

【００２２】なお、時刻証明書Ｃｔ（ｄ）には連結したデータ（ｄ＋ｐ）そのものではなく、利用者が利用できるそれぞれのデータに対するポインタや識別子でもよい。つまり、ポインタの先の情報が厳重に管理され、後から改ざんできないように管理されている場合には、データの構成のうち（ｄ＋ｐ）を（ｄへのポインタ＋ｐへのポインタ）に置き換えることにより、リソースの節約を図ることができる。

【００２３】以上のように、時刻証明書にタイムスタンプ機関１の電子署名Ｓｔ（ｄ＋ｐ）を含むため、タイムスタンプ機関１が情報ｄと公開情報ｐの関係を保証することとなる。公開情報ｐは、その事象が生じた日時がｔであることが周知であるか、あるいは第三者である情報公開機関３が公開情報ｐの発生日時ｔを保証するものであるため、単に数値データとして日時を添付するよりも直感的に日時を把握し易い。また、事前に予期できない情報を利用しているため、タイムスタンプ機関１が時刻証明書作成時ｔに偽ってｔ以降の時刻ｔ’を付与することはできない。つまり、時刻証明書が作成された日時が時刻証明書の示す日時以前でないことを確実に保証することができる。

【００２４】実施の形態２．以上の実施の形態では、時刻証明書を作成する際に時刻証明の対象となる情報と公開情報を利用したが、本実施の形態では、更に時刻情報を時刻証明書に含める。図４は、実施の形態２におけるブロック図である。図において、１～９は図１のものと同様であり、１０は、時刻情報を示すデータを生成する時刻データ生成手段である。

【００２５】次に動作について説明する。基本的な動作は実施の形態１と同様である。異なるのは、図２におけるステップ２とステップ３において、時刻データ生成手段１０により日時を示すデータｔを生成し、データ連結手段６によって時刻データｔを時刻証明の対象となる情報ｄと公開情報ｐと連結し、時刻ｔの情報を含む時刻証明書を生成するところである。これにより、情報ｄの時刻ｔに対する時刻証明書Ｃｔ（ｄ）には、タイムスタンプ機関１の電子署名Ｓｔ（ｔ＋ｄ＋ｐ）が含まれることになる。図５は、実施の形態２における時刻証明書Ｃｔ（ｄ）の構成を示す図である。

【００２６】以上のように、時刻データｔを含めることにより、時刻証明書から日時を直接認識することが可能である。また、必要に応じて、公開情報の示す日時と照合することにより、時刻データが示す日時の正否を確認できる。

【００２７】実施の形態３．以上の実施の形態では、タイムスタンプ機関は特に外部に情報も公開しないものであるが、本実施の形態では、タイムスタンプ機関が外部に対して情報公開する。

【００２８】図６は、実施の形態３におけるブロック図である。図６において、１～１０は図４のものと同様であり、１１は、時刻証明情報やその部分的な情報を公開する情報公開手段である。

【００２９】次に動作について説明する。図７は、実施の形態３における動作を示すフローチャートである。基本的な動作は、実施の形態２のものと一部を除いて同様であり、異なるのは図２におけるステップ１０３以降に

相当する部分のみである。まずステップ１１１で、利用者より利用者情報受信手段４により情報ｄを受ける。次にステップ１１２で、公開情報受信手段５により公開情報ｐを受ける。次にステップ１１３で、時刻情報性性手段１０により時刻を表すデータｔを生成する。次にステップ１１４で、データ連結手段６により、情報ｄのハッシュ値Ｈ（ｄ）を計算し、時刻ｔ、公開情報ｐと連結する。次にステップ１１５で、電子署名手段７により、電子署名Ｓｔ（ｔ＋Ｈ（ｄ）＋ｐ）を生成する。次にステップ１１６で時刻証明書出力手段８により電子署名Ｓｔ（ｔ＋Ｈ（ｄ）＋ｐ）と連結したデータ（ｔ＋Ｈ（ｄ）＋ｐ）を含む情報ｄに対する時刻証明書Ｃｔ（ｄ）を生成／出力する。図８は、実施の形態３における時刻証明書Ｃｔ（ｄ）の構成を示す図である。

【００３０】次に、情報公開手段１１により、連結したデータ（ｔ＋Ｈ（ｄ）＋ｐ）あるいはそのハッシュ値Ｈ（ｔ＋Ｈ（ｄ）＋ｐ）を含む情報を公開する。これらの情報を公開する手段は、例えば、ＣＤ－ＲＯＭに格納して配布する、定期刊行物に印刷して発行する、大手の新聞に掲載する、顧客や顧問弁護士に電子メールで送付するなどがある。

【００３１】以上のように、（ｔ＋Ｈ（ｄ）＋ｐ）を公開するようにしているので、情報ｄが時刻ｔに存在していたことを証明するために、周知にされた情報（ｔ＋Ｈ（ｄ）＋ｐ）を利用することによって説明することができる。情報ｄの秘匿性を保ちつつ、少なくとも情報ｄは（ｔ＋Ｈ（ｄ）＋ｐ）が公開された時刻ｔ１よりも以前に存在していたことが保証される。

【００３２】また、この公開情報を利用して自己あるいは他のタイムスタンプ機関が時刻証明書を生成できる。この場合、利用された公開情報に含まれる情報ｄがその公開情報を利用して生成された時刻証明書に含まれる情報ｄ１よりも早い時期に位置するものとして説明でき、更に同様の情報公開およびその公開情報の利用を繰り返すことにより、情報間の前後関係を改ざんすることが困難になり、情報ｄ，ｄ１，ｄ２・・・が時系列上に配置されることを保証できるようになる。

【００３３】実施の形態４．以上の実施の形態では、時刻証明の対象を無体物である情報としたものであるが、本実施の形態では、有体物に時刻証明をつける形態を説明する。図９は、実施の形態４におけるブロック図である。図９において、１，３，５～７，９，１０は図１のものと同様であり、１２は、公開情報と時刻情報を連結したデータとそれに対する署名をから、それらを含む情報を表す印刷形態（例えば、数値列、バーコード、あるいは図形など）を生成する時刻証明フォーマット生成手段、１３は、対象となる有体物に対して時刻証明フォーマット生成手段１２が生成した印刷形態を印刷する印刷手段である。

【００３４】次に動作について説明する。時間と共に変化する公開情報ｐと時刻データｔから電子署名手段７で電子署名Ｓｔ（ｔ＋ｐ）を生成するところまでは、連結や電子署名の対象に利用者端末２からの情報ｄを含めない点を除き、同様である。

【００３５】次に、時刻証明フォーマット生成手段１２が、公開情報ｐ、時刻データｔ、電子署名Ｓｔ（ｔ＋ｐ）から、人間あるいは機械が読み取れる形式（数字列、バーコード、図式表現など）を作成する。

【００３６】そして最後に、印刷手段１３により、時刻証明を付したい対象の有体物に印刷する。この時、容易に消去したり改ざんできない方法により印刷することが望ましい。また、時刻証明を有体物に直接印刷するのではなく、貼り換えの不可能なあるいは張り替えたことが容易に検知できるようなシールに印刷し、それを対象の有体物に貼り付けるようにしてもよい。

【００３７】以上のように、時間と共に変化する公開情報を含む時刻証明情報を対象物に印刷するようにしているので、時刻証明を与える者が予め未来の時刻を対象物に与えることができない。例えば、生鮮食料品に製造年月日や加工日時などを偽って未来の時刻を付しておき、顧客に対して新鮮であると誤解させることができなくなる。また、機械が読み取れる形式であるため、時刻証明を読み取り、署名の検証による改ざんチェックを行い、検証結果を表示するような装置が容易に実現できる。

【００３８】実施の形態５．実施の形態４は、時刻証明を生成し、それを有体物に添付する手段を示したものであるが、本実施の形態では、有体物に添付された時刻証明を検証する装置を示す。

【００３９】図１０は、時刻証明検証装置を示すブロック図である。１４は、時刻証明検証装置、１５は、機械が読み取れる形式（数字列、バーコード、その他の図式表現など）で印刷された時刻証明データを読み取る読み取り手段、１６は、読み取った時刻証明を検証する検証手段、１７は、検証結果を表示あるいは印刷する表示・印刷手段である。

【００４０】次に動作について説明する。まず、有体物に添付された機械が読み取れる形式（数字列、バーコード、その他の図式表現など）で印刷された時刻証明データを読み取り手段１５が読み取る。読み取ったデータには、公開情報ｐ、時刻データｔ、電子署名Ｓｔ（ｔ＋ｐ）が含まれる。次に、検証手段１６が、時刻データｔと公開情報ｐを連結したデータ（ｔ＋ｐ）と電子署名Ｓｔ（ｔ＋ｐ）により、電子署名検証を行なう。電子署名検証に用いる公開鍵は、検証を行なう機関が別途データベースに保管しておくか、あるいは第三者機関が認証書として発行しているものを用いる。

【００４１】また、検証手段１６は、電子署名検証の前あるいは後に、公開情報ｐの発生時刻を取得し、時刻データｔとの比較を行なう。公開情報ｐの発生時刻は、公開情報ｐを公開する機関に対してオンラインで照会する

ことにより、得られるものとする。照会の際には公開情報ｐを送付する。また、時刻データｔと公開情報ｐから得られた発生時刻に予め設定したしきい値以上の差がある場合には、時刻証明自体を信用しないこととし、検証を失敗することにする。

【００４２】次に、表示・印刷手段１７によって、検証が成功した場合は、時刻データｔをディスプレイに表示あるいは紙に印刷する。なお、本装置は商品の小売店が商品の販売時に利用するＰＯＳ端末に組込まれていてもよく、この時、読み取り手段１５は、時刻証明データと共に商品データを読み取り、検証結果を表示あるいは印刷する際に、小売店が管理するデータベースから引き出した該当する商品の名称と価格データと共に時刻データを表示し、レシートに印刷するようにしてもよい。

【００４３】以上のように、有体物に添付された時刻証明データを読み取り、検証し、表示・印刷するようにしているので、その有体物に時刻証明データが添付された時期が、付随する公開情報の発生時刻よりも後であることを保証し、それを利用者に示すことができる。図１１に、時間経過の概念を示す。また、時刻証明データには、時刻証明データの添付者の電子署名が付随するため、他の者が偽って異なった時刻証明データを添付することができない。従って、例えば、生鮮食料品の製造、発送、鶏卵の産出時刻、発送、調理品の製造等に対し、予め将来の時刻を偽って添付すること、あるいは小売店で新たな時刻証明を偽って添付することを防止できる。

【００４４】最後に、時刻証明書を用いる検証について補足する。検証としては、以下のように署名の検証、時刻の検証、情報の検証が行われる。

・署名の検証

時刻証明情報Ｃｔ（ｄ）の電子署名Ｓｔを検証する（実施の形態１，２，３）。

・時刻の検証

時刻証明情報Ｃｔ（ｄ）の時刻ｔを得る（実施の形態２，３のみ）。時刻証明情報Ｃｔ（ｄ）内の公開情報ｐの発生時刻を公開情報の情報源により確認する（実施の形態１，２，３）。

・情報の検証

時刻証明情報Ｃｔ（ｄ）の情報ｄを得る（実施の形態１，３のみ）。時刻証明情報Ｃｔ（ｄ）内の情報のハッシュ値Ｈ（ｄ）と情報ｄを照合する（実施の形態２のみ）。以上の検証を実施することにより、確認した時刻ｔには情報ｄが既に存在していたことを確認することができる。

【００４５】なお、上述の時刻は、原則として日付を含む概念であるが、証明のサイクルが短い場合には、日付を含まなくても有効なことがある。

【００４６】上述の時間情報設定装置及び時刻証明検証装置は、コンピュータであり、各要素は、プログラムにより処理を実行することができる。また、プログラムを記憶媒体に記憶させ、記憶媒体からコンピュータに読み取られるようにすることができる。

【００４７】

【発明の効果】本発明により、時刻情報を生成する際に、時刻情報を生成する時刻において、その時刻以降の時刻を表す時刻情報を生成できないことを保証することができる。また、時刻情報が表している時刻が、利用者に対して直感的にその当時の正しい時刻であることを認識させやすいものとすることができる。

【図面の簡単な説明】

【図１】　実施の形態１におけるブロック図である。

【図２】　実施の形態１におけるタイムスタンプ機関の動作を示すフローチャートである。

【図３】　実施の形態１における時刻証明書Ｃｔ（ｄ）の構成を示す図である。

【図４】　実施の形態２におけるブロック図である。

【図５】　実施の形態２における時刻証明書Ｃｔ（ｄ）の構成を示す図である。

【図６】　実施の形態３におけるブロック図である。

【図７】　実施の形態３における動作を示すフローチャートである。

【図８】　実施の形態３における時刻証明書Ｃｔ（ｄ）の構成を示す図である。

【図９】　実施の形態４におけるブロック図である。

【図１０】　時刻証明検証装置を示すブロック図である。

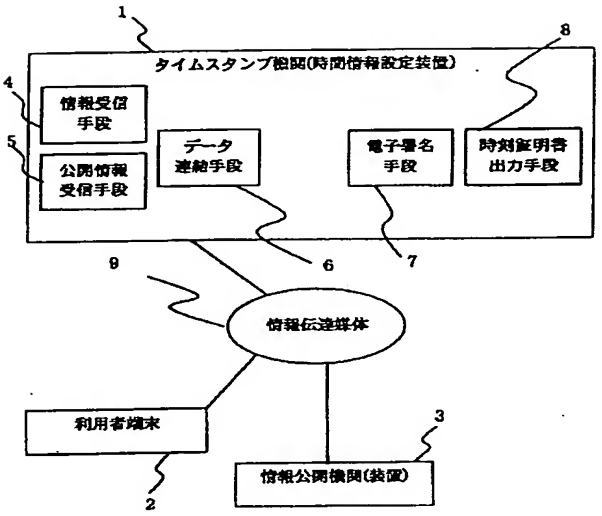
【図１１】　時間経過の概念を示す。

【図１２】　特表平６－５０１５７１に示された従来のタイムスタンプ方式のフローチャートを示している。

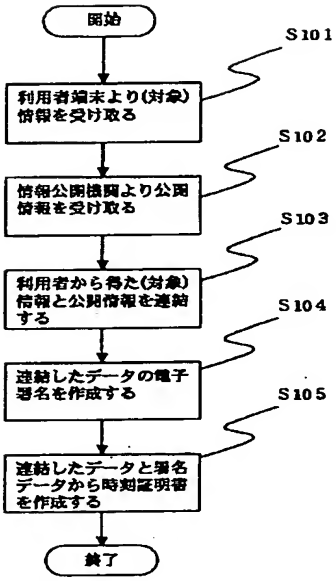
【符号の説明】

１　タイムスタンプ機関、２　利用者端末、３　情報公開機関、４　情報受信手段、５　公開情報受信手段、６　データ連結手段、７　電子署名手段、８　時刻証明出力手段、９　情報伝達媒体、１０　時刻データ生成手段、１１　情報公開手段、１２　時刻証明フォーマット生成手段、１３　印刷手段、１４　時刻証明検証装置、１５　読み取り手段、１６　検証手段、１７　表示・印刷手段。

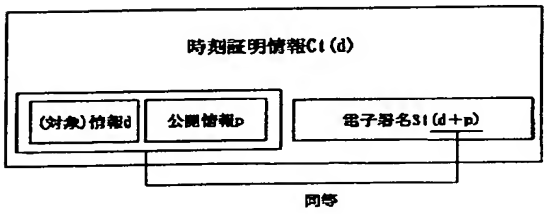
【図１】



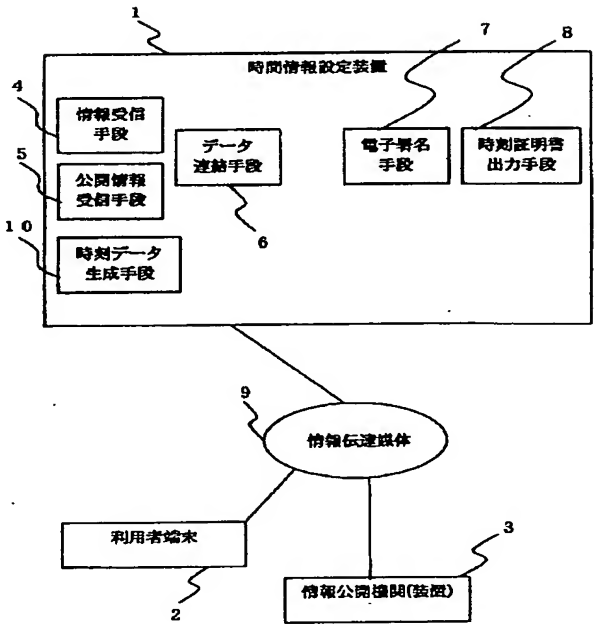
【図２】



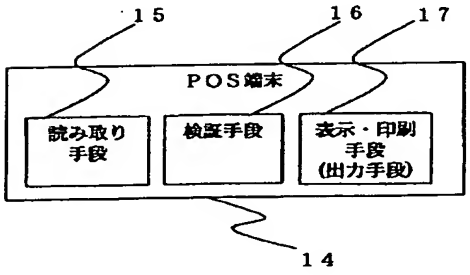
【図３】



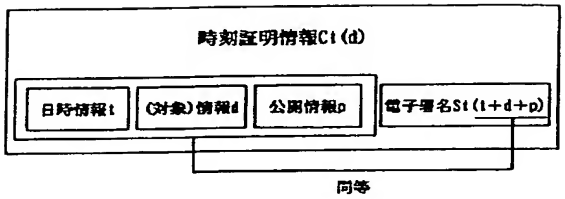
【図４】



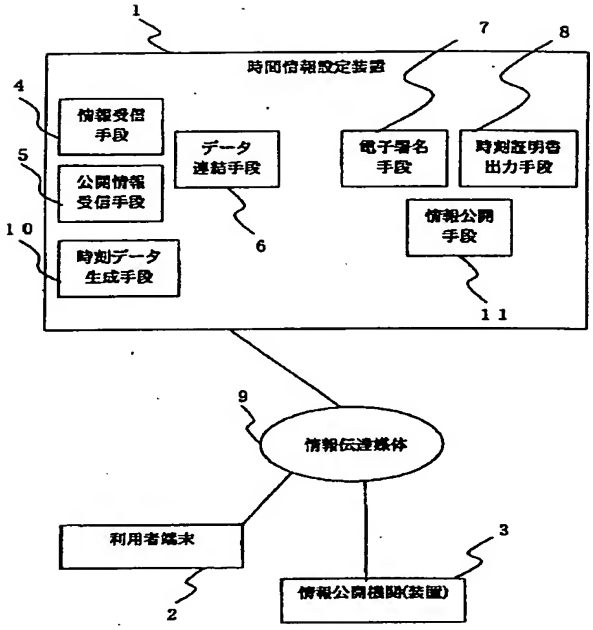
【図１０】



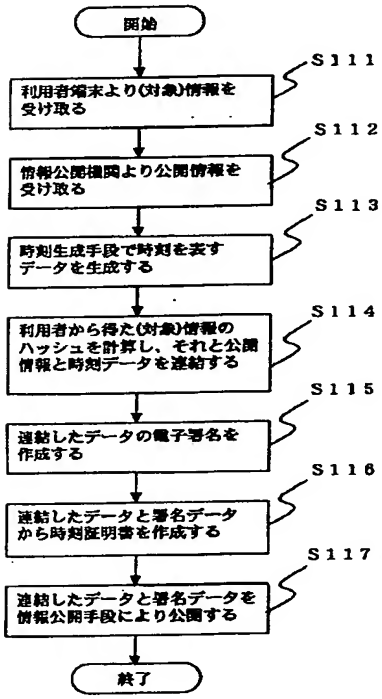
【図５】



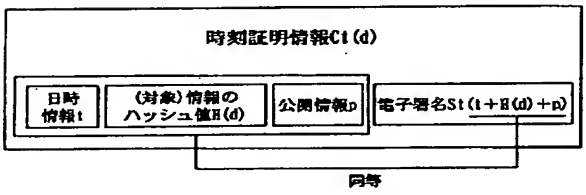
【図６】



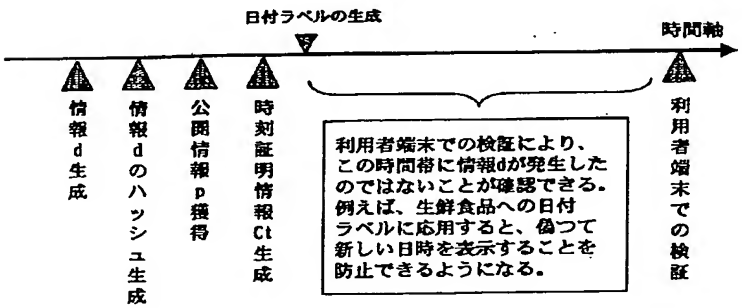
【図７】



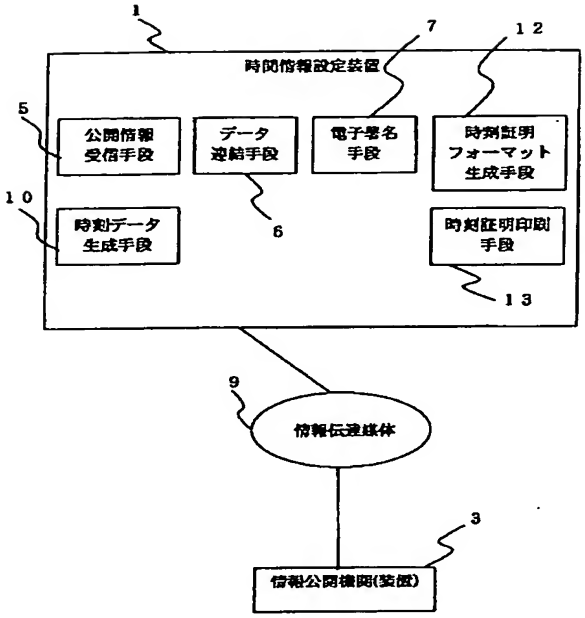
【図８】



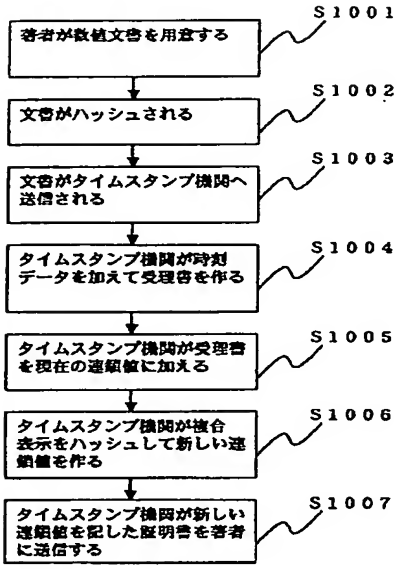
【図１１】



【図９】



【図１２】



フロントページの続き

(72)発明者　富樫　昌孝
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内

Ｆターム(参考)　5J104 AA09 AA11 LA06